DOI:
10.1016/j.jnt.2018.01.010

Document Version
Peer reviewed version

Frobenius elements in Galois representations with SL_n image

Matthew Bisatt

Faculty of Natural and Mathematical Sciences, Strand Campus, King's College London, London, WC2R 2LS, United Kingdom

Abstract

Suppose we have a elliptic curve over a number field whose mod l representation has image isomorphic to $\mathrm{SL}_2(\mathbb{F}_l)$. We present a method to determine Frobenius elements of the associated Galois group which incorporates the linear structure available. We are able to distinguish $\mathrm{SL}_n(\mathbb{F}_l)$-conjugacy from $\mathrm{GL}_n(\mathbb{F}_l)$-conjugacy; this can be thought of as being analogous to a result which distinguishes A_n-conjugacy from S_n-conjugacy when the Galois group is considered as a permutation group.

Suppose F is a number field and $f \in F[x]$ is an irreducible polynomial of degree n with splitting field K. How can we determine the $\mathrm{Gal}(K/F)$-conjugacy class of a Frobenius element, without explicitly constructing K? If we consider the Galois action on the roots, we can identify $\mathrm{Gal}(K/F)$ as a permutation group; the factorisation of f over the residue field enables us to find the cycle type of Frobenius and hence we have it up to conjugacy in the symmetric group S_n. If the Galois group is isomorphic to the alternating group A_5 though, then this is insufficient if f remains irreducible since there are two different conjugacy classes of 5-cycles in A_5. Serre [2, p.53] observed that computing a "square root" of the discriminant of f produced the extra necessary data. Roberts [8] then considered all alternating groups before Dokchitser and Dokchitser [5] generalised this to any finite group by constructing suitable resolvents.

In number theory, Galois extensions also arise from Galois representations; in this setting we have a natural linear action on the underlying vector space. Indeed, all current applications of the algorithm of Dokchitser and Dokchitser are to matrix groups [4, 7, 11, 12]. We wish to incorporate this extra structure so instead embed the Galois

group into a matrix group as opposed to a permutation group to yield an alternative approach to the problem of distinguishing Frobenius elements. We shall not give a complete theory for differentiating conjugacy classes of an arbitrary matrix group, but consider an analogue of the S_n versus A_n situation: $\mathrm{GL}_n(\mathbb{F}_l)$ versus $\mathrm{SL}_n(\mathbb{F}_l)$, where l is a rational prime. We illustrate our approach with the aid of elliptic curves, using the Weil pairing for our additional information. For the remainder of the paper, we shall abbreviate $\mathrm{SL}_2(\mathbb{F}_l)$ and $\mathrm{GL}_2(\mathbb{F}_l)$ to SL_2 and GL_2 respectively and say the GL_2-conjugacy class of an element $\sigma \in \mathrm{SL}_2$ *splits* if its SL_2-conjugacy class is properly contained in its GL_2-conjugacy class.

Let E/F be an elliptic curve and fix a rational prime l. Then the action of $\mathrm{Gal}(\overline{F}/F)$ on the group $E[l]$ of l-torsion points gives rise to the mod l Galois representation

$$\rho_{E,l} : \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_2(\mathbb{F}_l),$$

which factors through $\mathrm{Gal}(K/F)$, where K is the smallest extension of F over which all l-torsion points are defined. Let $\mathfrak{p}$ be a prime of F which is unramified in K and does not divide the discriminant Δ_E of E (it suffices to assume $\mathfrak{p} \nmid l\Delta_E$; this is the assumption we will generally use).

There are two standard pieces of information that we can acquire about the Frobenius element coming from its characteristic polynomial. Firstly, the determinant is equal to the absolute norm q of $\mathfrak{p}$. We can also ascertain its trace by examining the number of points on the reduced curve (see for example Schoof's algorithm [9] or the refined Schoof-Elkies-Atkin algorithm).

Unfortunately, these two pieces of data do not always completely distinguish the conjugacy class, even in GL_2. When it is difficult to establish the GL_2-class, we note that Duke and Tóth [6, Thm 2.1] give a method for determining this. Sutherland takes a different approach in [10] to compute the entire Galois image by sampling various Frobenius elements; the need to determine their individual conjugacy classes also arises here.

Remark 1. *We shall suppose that* $\mathrm{Im}\,\rho_{E,l} = \mathrm{SL}_2$*, which implies that the* F *contains a primitive* l^{th} *root of unity* ζ_l *and* $q \equiv 1 \bmod l$*. Recall that if* $\zeta_l \in F$ *and* E *is an elliptic curve without complex multiplication, then* $\mathrm{Im}\,\rho_{E,l} = \mathrm{SL}_2$ *is true for all but finitely many primes* l *by Serre's open image theorem.*

We now give a further criterion to distinguish between two classes in SL_2 that are conjugate in GL_2 and define $\mathrm{GL}_2^{\square} := \{A \in \mathrm{GL}_2 \mid \det A \text{ is a square } \}$.

Theorem 2. *Let E/F be an elliptic curve such that $\rho_{E,l}(\mathrm{Gal}(\overline{F}/F)) = \mathrm{SL}_2$ and $\mathfrak{p}$ be a prime of F of absolute norm q such that $\mathfrak{p} \nmid l\Delta_E$. Let $\sigma \in \mathrm{SL}_2$ be GL_2-conjugate to $\rho_{E,l}(\mathrm{Frob}_{\mathfrak{p}})$ and suppose that the GL_2-conjugacy class of σ splits in SL_2.*

Let $\tilde{E}$ be the reduced curve at $\mathfrak{p}$ and suppose that (Q_1, Q_2) is an ordered basis of $\tilde{E}[l]$ such that the action of the Frobenius automorphism $x \mapsto x^q$ acts as $\sigma \in \mathrm{SL}_2$ on $\tilde{E}[l]$ with respect to (Q_1, Q_2).

Then $\rho_{E,l}(\mathrm{Frob}_{\mathfrak{p}})$, written with respect to a global ordered basis (P_1, P_2), is SL_2-conjugate to σ if and only if

$$\langle P_1, P_2\rangle_l \mod \mathfrak{p} \equiv \langle Q_1, Q_2\rangle_l^{k^2} \text{ for some } k \in \mathbb{Z},$$

where $\langle\ ,\ \rangle_l$ denotes the Weil pairing.

Proof. Write $\rho_{E,l}(\mathrm{Frob}_{\mathfrak{p}}) = \tau$ (with respect to P_1, P_2) and let $P_i' \in E[l]$ be such that $P_i' \bmod \mathfrak{p} = Q_i$ for $i = 1, 2$. First suppose that $\tau = \sigma$. If $P_i = P_i', i = 1, 2$, then the result trivially holds. Otherwise the possible ordered bases which give also give τ are in bijection with elements in the GL_2-centraliser $C_{\mathrm{GL}_2}(\sigma)$. By the orbit-stabiliser theorem, we can compute that the SL_2-centraliser of σ, $C_{\mathrm{SL}_2}(\sigma)$ has index $\frac{2}{l-1}$ in its GL_2-centraliser (as we impose that the SL_2-class splits) and moreover, $C_{\mathrm{GL}_2}(\sigma) = ZC_{\mathrm{SL}_2}(\sigma) \subset \mathrm{GL}_2^{\square}$, where Z is the centre of GL_2 which consists of scalar matrices.

Now suppose $\tau \neq \sigma$. By assumption, τ is GL_2-conjugate to σ so there exists $A \in \mathrm{GL}_2$ such that $\sigma = A^{-1}\tau A$. We claim that τ is SL_2-conjugate to σ if and only if $A \in \mathrm{SL}_2 C_{\mathrm{GL}_2}(\sigma) = \mathrm{GL}_2^{\square}$. Assume first that $A = A_1A_2$ with $A_1 \in \mathrm{SL}_2$, $A_2 \in C_{\mathrm{GL}_2}(\sigma)$. Then $A_1^{-1}\tau A_1 = \sigma$ and we are done. Conversely, suppose σ, τ are SL_2-conjugate and write $\sigma = B^{-1}\tau B$ with $B \in \mathrm{SL}_2$. Then $B^{-1}A \in C_{\mathrm{GL}_2}(\sigma)$ which proves the claim.

Let α be the matrix that maps P_i' to $P_i, i = 1, 2$. Then $\langle P_1, P_2\rangle_l = \langle \alpha(P_1'), \alpha(P_2')\rangle_l = \langle P_1', P_2'\rangle_l^{\det \alpha} \bmod \mathfrak{p} \equiv \langle Q_1, Q_2\rangle^{\det \alpha}$. Then by the above argument, τ (with respect to P_1, P_2) is SL_2-conjugate to σ (with respect to Q_1, Q_2) if and only if $\alpha \in \mathrm{GL}_2^{\square}$ which completes the proof. □

Remark 3. *To discuss conjugacy questions about the image, it is necessary to fix a global basis as a reference point. In principle, one could then simply take the local basis to be the reduction of the global one; the GL_2-conjugacy class then suffices to determine the SL_2 class.*

However, determining a global basis precisely enough is computationally expensive for large l so this is far from ideal. In practice, we use the lattice interpretation of the elliptic curve; this enables us to compute a global basis as points in $E(\mathbb{C})$ (together with their Weil pairing) with minimal effort. This approach simplifies the global calculation but prevents us from computing their images in the residue field easily, which is where we then apply our theorem to distinguish conjugacy.

We do not actually need the image to be SL_2 to apply the above theorem. However, F may not contain the relevant roots of unity so to combat this we should consider the minimal polynomials.

Let $m_F(\alpha)$ denote the minimal polynomial of α over F, for any field F and algebraic number α.

Theorem 4. *Let E/F be an elliptic curve and let $\rho_{E,l}(\mathrm{Gal}(\overline{F}/F)) = G \subset \mathrm{GL}_2$. Let $\mathfrak{p}$ be a prime of norm q such that $\mathfrak{p} \nmid l\Delta_E$ and $q \equiv 1 \bmod l$. Let $\sigma \in \mathrm{SL}_2$ be GL_2-conjugate to $\rho_{E,l}(\mathrm{Frob}_\mathfrak{p})$ and suppose that the G-conjugacy class of σ is equal to the intersection of G with its SL_2-conjugacy class.*

Let $\tilde{E}$ be the reduced curve at $\mathfrak{p}$ and suppose that (Q_1, Q_2) is an ordered basis of $\tilde{E}[l]$ such that the action of the Frobenius automorphism $x \mapsto x^q$ acts as σ on $\tilde{E}[l]$ with respect to (Q_1, Q_2).

Then $\rho_{E,l}(\mathrm{Frob}_\mathfrak{p})$, written with respect to a global ordered basis (P_1, P_2), is G-conjugate to σ if and only if

$$m_\mathcal{F}(\langle Q_1, Q_2\rangle_l^{k^2}) \text{ divides } m_F(\langle P_1, P_2\rangle_l) \bmod \mathfrak{p}$$

for some $k \in \mathbb{Z}$, where $\mathcal{F}$ is the residue field of F at $\mathfrak{p}$.

Proof. By the assumption on G, $\rho_{E,l}(\mathrm{Frob}_\mathfrak{p})$ is G-conjugate to σ if and only if it is SL_2-conjugate to σ, with respect to the same global ordered basis (P_1, P_2). Let $L = F(\zeta_l)$. Then for any prime $\mathfrak{P}$ of L above $\mathfrak{p}$, we have that $\rho_{E,l}(\mathrm{Frob}_\mathfrak{P})$, with respect to (P_1, P_2), is G-conjugate to σ if and only if $\langle Q_1, Q_2\rangle_l^{k^2} \equiv \langle P_1, P_2\rangle_l \bmod \mathfrak{P}$ for some $k \in \mathbb{Z}$ by Theorem 2.

As $q \equiv 1 \bmod l$, $\mathfrak{p}$ splits completely in L hence $\mathrm{Frob}_\mathfrak{P} = \mathrm{Frob}_\mathfrak{p}$. Moreover, $m_\mathcal{F} = m_\mathcal{F}(\langle Q_1, Q_2\rangle_l^{k^2})$ is linear and $m_F = m_F(\langle P_1, P_2\rangle_l) = \prod_{g \in \mathrm{Gal}(L/F)} (x - g(\langle P_1, P_2\rangle_l))$. It remains to show $m_\mathcal{F}$ divides $m_F \bmod \mathfrak{p}$ if and only if $\langle Q_1, Q_2\rangle_l^{k^2} \equiv \langle P_1, P_2\rangle_l \bmod \mathfrak{P}$ for some choice of $\mathfrak{P}|\mathfrak{p}$.

Suppose $\langle Q_1, Q_2\rangle_l^{k^2} \equiv \langle P_1, P_2\rangle_l \bmod \mathfrak{P}$. As $m_\mathcal{F}$ is linear, we have divisibility $\bmod \mathfrak{P} \cap F = \mathfrak{p}$. Conversely, fix $\mathfrak{P}$ and suppose $m_\mathcal{F}$ divides $m_F \bmod \mathfrak{p}$. Then $\langle Q_1, Q_2\rangle_l^{k^2} \equiv g(\langle P_1, P_2\rangle_l) \bmod \mathfrak{P}$ for some $g \in \mathrm{Gal}(L/F)$ and hence $\langle Q_1, Q_2\rangle_l^{k^2} \equiv \langle P_1, P_2\rangle_l \bmod g^{-1}(\mathfrak{P})$. □

Example 5. *Let $E/\mathbb{Q}(\zeta_3)$ be the elliptic curve $y^2 = x^3 + x + 1$ (Cremona label 496a1), where $\zeta_3 = e^{2\pi i/3}$. The image of the mod 3 representation of $E/\mathbb{Q}(\zeta_3)$ is isomorphic to $\mathrm{SL}_2(\mathbb{F}_3)$. Let $\mathfrak{p} = (13, \zeta_3 - 3)$ be a prime of $\mathbb{Q}(\zeta_3)$. We shall compute the SL_2-conjugacy class of $\rho_{E,3}(\mathrm{Frob}_\mathfrak{p})$.*

Choose a global basis $P_1 = (\alpha_1, \beta_1), P_2 = (\overline{\alpha_1}, \overline{\beta_1}) \in E(\mathbb{C})$, where $\alpha_1 \approx 0.571 + 1.754i, \beta_1 \approx 0.984 + 2.761i$ and observe that $\langle P_1, P_2\rangle_3 = \zeta_3$.

Now the reduced curve $\tilde{E}$ has 18 points so the trace of Frobenius is $2 \bmod 3$, hence the image of Frobenius (with respect to (P_1, P_2)) is SL_2-conjugate to $\left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$ for some $n \in \{0, 1, 2\}$. These all define distinct SL_2-conjugacy classes, with the non-identity elements being GL_2-conjugate.

A quick check shows that $\tilde{E}(\mathbb{F}_{13})[3] \neq 9$ *hence* $n \neq 0$ *so* $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$ *is* GL_2*-conjugate to* $\rho_{E,3}(\mathrm{Frob}_{\mathfrak{p}})$.

Now $\tilde{E}[3]$ *is defined over the cubic extension* $\mathbb{F}_{13}[\alpha]$*, where* α *has minimal polynomial* $x^3 + 2x - 2$*. We compute that* $Q_1 = (10, 6)$*,* $Q_2 = (8\alpha^2 - \alpha + 3, 7\alpha^2 + 4\alpha - 1)$ *is a basis of* $\tilde{E}[3]$ *such that the Frobenius automorphism acts as* $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$ *here.*

The criterion we have in this case is equivalent to checking whether $\langle P_1, P_2\rangle_3 \equiv \langle Q_1, Q_2\rangle_3 \bmod \mathfrak{p}$*. A quick calculation shows that* $\langle Q_1, Q_2\rangle_3 = 3$ *so* $\rho_{E,3}(\mathrm{Frob}_{\mathfrak{p}})$ *is* SL_2*-conjugate to* $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$ *with respect to* (P_1, P_2).

Example 6. *Consider the elliptic curve* $y^2 + y = x^3 - x^2$ *(Cremona label 11a3) defined over* $\mathbb{Q}(\sqrt{5})$*. The mod* 5 *image is isomorphic to* D_{10}*, the dihedral group of order 10 generated by* $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$ *and* $\left(\begin{smallmatrix}1 & 0\\ 0 & 4\end{smallmatrix}\right)$ [1]*. This is not contained in* $\mathrm{SL}_2(\mathbb{F}_5)$ *but the order* 5 *elements satisfy the conditions of Theorem 4.*

Let $\mathfrak{p} = (\frac{1+5\sqrt{5}}{2})$ *be a prime of* $\mathbb{Q}(\sqrt{5})$ *above* 31*. Choose the ordered global basis* $P_1 \approx (1.69 - 1.54i, -1.27 + 2.83i), P_2 = (1, -1)$ *so* $\langle P_1, P_2\rangle_5 = e^{2\pi i/5}$*. This is not an element of* $\mathbb{Q}(\sqrt{5})$ *so we instead take its minimal polynomial* $m_{\mathbb{Q}(\sqrt{5})}(e^{2\pi i/5}) = x^2 + \frac{1}{2}(1 + \sqrt{5})x + 1$.

One can check that $\mathrm{Frob}_{\mathfrak{p}}$ *has order* 5 *using the group structure of the reduced curve and so is conjugate to either* $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$ *or* $\left(\begin{smallmatrix}1 & 2\\ 0 & 1\end{smallmatrix}\right)$ *under the ordered basis* (P_1, P_2).

Let $Q_1 = (1, -1), Q_2 = (26\alpha^3 + 8\alpha^2 + 23\alpha + 12, 16\alpha^4 + 17\alpha^3 + 29\alpha^2 + 17\alpha + 2)$*, where* α *has minimal polynomial* $x^5 + 7x + 28$*. Then the Frobenius automorphism acts on* $\tilde{E}[5]$ *as* $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$ *with respect to the ordered basis* (Q_1, Q_2).

We compute that $\langle Q_1, Q_2\rangle_5 = 8$*. Now* $m_{\mathbb{Q}(\sqrt{5})}(e^{2\pi i/5}) \equiv x^2 + 13x + 1 \bmod \mathfrak{p}$ *which does not have* 8 *as a root so* $\mathrm{Frob}_{\mathfrak{p}}$ *cannot be conjugate to* $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$*. Redoing the calculation with* $\left(\begin{smallmatrix}1 & 2\\ 0 & 1\end{smallmatrix}\right)$*, (where we take the basis* $(Q_1, Q_1 + 2Q_2)$*), the Weil pairing is* 2 *which is a root of* $m_{\mathbb{Q}(\sqrt{5})}(e^{2\pi i/5}) \bmod \mathfrak{p}$*. Hence* $\mathrm{Frob}_{\mathfrak{p}}$ *is* D_{10}*-conjugate to* $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$ *with respect to the basis* (P_1, P_2).

Remark 7. *We ran our method against the current algorithm of Dokchitser and Dokchitser in Magma. Their algorithm is not yet implemented over number fields so we only ran ours for rational primes which were completely split in the base field so the Frobenius element is unchanged. In addition, the bulk of the computation in their method consists of constructing a polynomial for each conjugacy class first. For a fairer comparison, we chose to time the results to determine the Frobenius elements at 1000 suitable rational primes in the mod* $3, 5, 7$ *and* 11 *representations of the elliptic curve* $y^2 = x^3 + x + 1$*; the computation was run on a machine with an AMD Opteron(tm) Processor 6174 and a speed of 2200MHz. We tabulate our results below.*

l	*Weil Pairing Method*	*Dokchitsers' Method*
3	5.7 *seconds*	0.5 *seconds*
5	25.7 *seconds*	11.4 *seconds*
7	88.7 *seconds*	1032.3 *seconds*
11	373.4 *seconds*	> 7 *days*

[1] The mod 5 image was obtained from [3, elliptic curve 11.a3] at `http://www.lmfdb.org/EllipticCurve/Q/11/a/3`, using data computed via methods in [10].

The final thing we wish to address is how beneficial elliptic curves were here as to the feasibility of this method for Galois representations arising from other types of objects. We can also do this for larger dimensional vector spaces, so we will incorporate this into our theorem.

We first recall a construction which generalises the precise properties of the Weil pairing that we want. Let $V/\mathbb{F}_l$ be a vector space of dimension n. Then the n^{th} exterior power $\Lambda^n V^*$ is a one dimensional vector space of alternating multilinear forms, such that for any nonzero $T \in \Lambda^n V^*$ we have

1. $T(v_1, \cdots, v_n) = 0$ if and only if $\{v_1, \cdots, v_n\}$ are linearly dependent,
2. $T(Av_1, \cdots, Av_n) = \det(A)T(v_1, \cdots, v_n)$ for all matrices $A \in \mathrm{GL}_n(\mathbb{F}_l)$.

In the case of the Weil pairing, we identified the image $\mathbb{F}_l$ with the l^{th} roots of unity and shall do so again in our final theorem. For a field F, we let $\mu_l(F)$ denote the l^{th} roots of unity in F.

Theorem 8. *Let K/F be a Galois extension of number fields, such that $\rho : \mathrm{Gal}(K/F) \to \mathrm{SL}_n(\mathbb{F}_l)$ is an isomorphism for some rational prime l and positive integer n. Let $\mathfrak{p}$ be a prime of F which is unramified in K and $\mathfrak{P}$ a prime of K above $\mathfrak{p}$ with corresponding residue fields $\mathcal{F}$ and $\mathcal{K}$. Write $G = \mathrm{Gal}(K/F)$ and $\overline{G} = \mathrm{Gal}(\mathcal{K}/\mathcal{F})$, where we identify the latter with the decomposition subgroup.*

Let $V, \overline{V}$ be two $\mathbb{F}_l$-vector spaces of dimension n. Suppose V (respectively $\overline{V}$) has a faithful action of G (respectively $\overline{G}$) and there exists an isomorphism $\theta : V \to \overline{V}$ such that $\theta\overline{g} = \overline{g}\theta$ for all $\overline{g} \in \overline{G}$. Furthermore, suppose that there are nonzero alternating multilinear forms $T_F \in \Lambda^n V^*$ and $T_{\mathcal{F}} \in \Lambda^n \overline{V}^*$ such that the diagram

$$\begin{array}{ccc} V^n & \xrightarrow{T_F} & \mu_l(F) \\ \downarrow{\scriptstyle \tilde{\theta}} & & \downarrow{\scriptstyle \mathrm{mod}\ \mathfrak{p}} \\ \overline{V}^n & \xrightarrow{T_{\mathcal{F}}} & \mu_l(\mathcal{F}) \end{array}$$

commutes, where $\tilde{\theta}(v_1, \cdots, v_n) := (\theta(v_1), \cdots, \theta(v_n))$.

Suppose the $\mathrm{GL}_n(\mathbb{F}_l)$-conjugacy class of $\rho(\mathrm{Frob}_{\mathfrak{p}})$ splits into m classes in $\mathrm{SL}_n(\mathbb{F}_l)$ and let $H \subset \mathbb{F}_l^\times$ be the unique subgroup such that $[\mathbb{F}_l^\times : H] = m$. Suppose $\sigma \in \mathrm{SL}_n(\mathbb{F}_l)$ is $\mathrm{GL}_n(\mathbb{F}_l)$-conjugate to $\rho(\mathrm{Frob}_{\mathfrak{p}})$ and let $\overline{B}$ be an ordered basis of $\overline{V}$ such that the Frobenius automorphism acts as σ on $\overline{V}$ with respect to $\overline{B}$. Then $\rho(\mathrm{Frob}_{\mathfrak{p}})$, written with respect to a global ordered basis B, is $\mathrm{SL}_n(\mathbb{F}_l)$-conjugate to σ if and only if

$$T_F(B) \mod \mathfrak{p} \equiv T_{\mathcal{F}}(\overline{B})^h \qquad \text{for some } h \in H.$$

Proof. Let $B' = \tilde{\theta}^{-1}(\overline{B})$ and suppose first that $\tau = \sigma, B = B'$. Then $T_F(B) = T_F(\tilde{\theta}^{-1}(\overline{B}))$ and the result follows from the commutativity of the diagram.

Otherwise, we mimic the proof of Theorem 2, where this time $[C_{\mathrm{GL}_n(\mathbb{F}_l)}(\sigma) : C_{\mathrm{SL}_n(\mathbb{F}_l)}(\sigma)] = \frac{m}{l-1}$. Recall that for a normal subgroup N of a group M, the splitting of an M-conjugacy class of $n \in N$ in N is in bijection with the coset space over the centraliser $M/NC_M(n)$. In our situation this bijection is between the splitting of the $\mathrm{GL}_n(\mathbb{F}_l)$ conjugacy class of σ in $\mathrm{SL}_n(\mathbb{F}_l)$ and the subgroup $\mathbb{F}_l^\times / \det C_{\mathrm{GL}_n(\mathbb{F}_l)}(\sigma)$.

Therefore $\det C_{\mathrm{GL}_n(\mathbb{F}_l)}(\sigma) = H$ so $C_{\mathrm{GL}_n(\mathbb{F}_l)}(\sigma) \subset GL_n^H(\mathbb{F}_l) = \{A \in \mathrm{GL}_n(\mathbb{F}_l) | \det A \in H\}$. Moreover, if $A \in \mathrm{GL}_n(\mathbb{F}_l)$ is such that $\sigma = A^{-1}\tau A$, then σ, τ are $\mathrm{SL}_n(\mathbb{F}_l)$-conjugate if and only if $A \in \mathrm{SL}_n(\mathbb{F}_l) C_{\mathrm{GL}_n(\mathbb{F}_l)}(\sigma) = GL_n^H(\mathbb{F}_l)$. The result now follows from the fact that $T_F(\alpha B) = T_F(B)^{\det \alpha}$ for any $\alpha \in \mathrm{GL}_n(\mathbb{F}_l)$. □

Acknowledgements. *I wish to thank Vladimir Dokchitser for many useful discussions, as well as Tim Dokchitser and Andrew Sutherland for their comments. I would also like to thank both the University of Warwick and King's College London where this research was carried out. This research was funded by an EPSRC studentship.*

[1] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24:235–265, 1997.

[2] J. Buhler. *Icosahedral Galois representations*, volume 654. Springer-Verlag, 1978.

[3] LMFDB Collaboration. The L-functions and modular forms database. *http://www.lmfdb.org*, 2017.

[4] L. Dembélé, F. Diamond, and D. Roberts. Serre weights and wild ramification in two-dimensional Galois representations. *Forum of Mathematics, Sigma*, 4, 2016.

[5] T. Dokchitser and V. Dokchitser. Identifying frobenius elements in Galois groups. *Algebra and Number Theory*, 7(6):1325–1352, 2013.

[6] W. Duke and A. Tóth. The splitting of primes in division fields of elliptic curves. *Experimental Mathematics*, 11(4):555–565, 2002.

[7] N. Mascot. Computing modular Galois representations. *Rendiconti del Circolo Matematico di Palermo*, 62(3):451–476, 2013.

[8] D. Roberts. Frobenius classes in alternating groups. *Rocky Mountain J. Math*, 34(4):1483–1496, 2004.

[9] R. Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Mathematics of Computation*, 44(170):483–494, 1985.

[10] A. Sutherland. Computing images of Galois representations attached to elliptic curves. *Forum of Mathematics, Sigma*, 4:e4, 2016.

[11] L. Yin and J. Zeng. On the computation of coefficients of modular forms: the reduction modulo p approach. *Mathematics of Computation*, 84, 2015.

[12] J. Zeng. Computing Galois representations of modular abelian surfaces. *LMS Journal of Computation and Mathematics*, 17(A):36–48, 2014.